Guide to Risk Assessments

Introduction

Risk is defined as the potential for loss, damage, or destruction of key resources or power system assets resulting from a threat. Risk is evaluated as the product of the threat likelihood and vulnerability severity scores. Analyzing risk is a key step in vulnerability assessments and allows for the prioritization of vulnerability mitigation actions. This document presents the steps involved in analyzing risks:

- Assess risks
- Score risks
- Evaluate risks
- Identify levels of risk acceptance

Risk—the potential for loss, damage, or destruction of power system assets or other key resources resulting from a *threat*. Risk is evaluated as the product of the *threat likelihood score* and the *vulnerability severity score.*

1. Assess Risks

Not all threats directly influence each vulnerability. As such, the first step involves determining which threats and vulnerabilities are associated. The matrix shown in Figure 2 is one way to do this.

2. Score Risks

There are many different methodologies for scoring risk. The method highlighted here is based on that developed by Anderson et al, 2018, and uses risk matrices to score and prioritize risks. Risk matrices show the relationships between threats and vulnerabilities. The severity score for each vulnerability is multiplied by the threat likelihood score to create a risk score for each specific threat-vulnerability combination. Risk scores are scaled from one to 100, with higher scores corresponding to higher risks. This requires assigning quantitative values to the qualitative thresholds previously presented in

	VULNERABILITIES								
THREATS	Infrastructure design susceptible to failure	Aging infrastructure	Undersized power systems	Lack of redundant generation for at least 30% of load	Lack of operational flexibility	Lack of capital for system upgrades	Lack of properly trained workforce	Lack of coordination with other government agencies	No formal disaster or emergency plans in IRRP
More frequent flooding	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Increased annual average temperature	Yes	Yes	Yes	No	Yes	No	No	No	No
Increased intensity of typhoon winds	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Increased number of days with thunderstorms/lightning	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Typhoons	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Increased landslides	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Increase in magnitude of hottest annual temperature	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Increased change of drought/low water levels	No	No	No	No	Yes	Yes	No	Yes	Yes
Increased number of days with 95°F (35°C) or higher per year	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Increased number of days with heavy rainfall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Increased precipitation on days with precipitation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Infrastructure failure	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Figure 2. Example matrix linking threats to vulnerabilities

the threat and vulnerability sections of this guidebook. The risk is calculated as:

Risk score = Threat likelihood score X Vulnerability severity score

Developing a risk matrix provides a structure for combining scores in a meaningful way that enables analysis and ranking of the risks to prioritize mitigation actions. No risk score is assigned where threats are not associated with a vulnerability, and the matrix is blank at this intersection. The final risk score is shown in the matrix and used to prioritize the vulnerabilities (Figure 3).

3. Evaluate Risks

The heat map (Figure 3) portrays high-risk scores as red cells (top left) and low-risk scores as orange or yellow values (bottom right). Blank cells indicate a lack of connection between that combination of a threat and vulnerability. This format helps in displaying the relative importance of different risks and provides insight into potential causes of—and vulnerabilities to—disruptive events. This can also enable decision makers to identify tailored resilience solutions for certain vulnerability-threat combinations. For example, a decision maker could weigh specific vulnerabilities against the likelihood of different threats and be well-positioned to direct resources to priority areas.

		THREATS												
		Extreme Precipitation	Extreme Temperatures	Flooding	Landslides	Wildfire Interactions	Wind	Human Actions: Bad Actors	Human Actions: Accidents	Technological Design	Technological Materials	Technological Workmanship	Drought	Lightning
		Threat Likelihood Score												
VULNERABILITIES	Vulnerability Severity Score	9	7	7	7	5	5	5	5	5	5	5	5	1
Power system rules, regulations, and technical standards do not meet current and changing environmental conditions	9	81		63	63			45		45	45			
Corruption leads to code violations	9	81			63	45	45	45			45	45		
Dam construction does not follow design specifications	9	81	63		63	45	45	45	45	45	45	45		
Installation does not follow design specifications	9			63	63	45		45	45	45		45		
Lack of compliance with codes in design	9	81	63	63	63	45	45			45	45	45		
System operations are not flexible enough to respond to changes in demand and supply	7	63	49	49			35			35			35	7
Demand forecasting is not responsive to changing load conditions	7	63	49							35			35	
Heavy power sector reliance on hydro generation	7		49	49						35			35	
Inadequate domestic generation capacity requires costly energy imports	7		49	49	49	35	35	35	35	35	35	35	35	

Figure 3. Example risk matrix

4. Identify levels of risk acceptance

A comprehensive risk evaluation will likely yield far more threat-vulnerability pairs than can be addressed. In this case, the next step of the assessment involves using experience and professional judgment to form a plan for how many and on which of these pairs to focus. Making these decisions serves to identify what threshold of risk is tolerable and possible, and which threat-vulnerability pairs are critical and feasible to address.

In this decision-making process, some factors to consider are:

- Which vulnerabilities are affected by the largest number of risks?
- Whether priority will be given to the high-frequency risks or the highest-impact risks.
- What level of risk is the power sector capable of realizing—financially, technologically, and logistically?

After the decision makers have identified these levels of risk acceptance and focused their list of priorities, they should be sure to re-engage relevant stakeholders for feedback, amendments, and approval.